DOI: 10.18372/2307-9061.72.19062
УДК 340.5(045)

A. Samakashvili,
Master of Law of Sokhumi State University,
Deputy Director of the «Tbilisi Sports and Youth Center»

TECHNOLOGY AND LEGAL CHALLENGES OF CONTEMPORARY ARMED CONFLICT

Sokhumi State University
Ana Politkovskaia St, PPC5+6GG, Tbilisi, Georgia
E-mail: ana.samakashvili@sou.edu.ge

The purpose *of the article is to research the relationship between IHL, IHRL and national law norms, and to give recommendations about the prevention of using technologies in contemporary armed conflicts.* ***Research methods:*** *in the article, the research was carried out using the comparative-legal method in order to present the relationship between international and national legal norms. Also, we will use the normative method to emphasize the need of introduction of new norms to regulate the problem.* ***Results:*** *after the World War II, adoption of the new international norms significantly decreased the war statistics, however, in recent years, development of technologies, which was further accelerated by the pandemic, changed the mentioned statistics, to the extent that new technologies are actively used in war. Unfortunately, preventive and/or prohibitive international norms do not exist, therefore, we do not have the practice of regulating them. Paucity of regulative norms and the absence of proper literature in this field underscores the relevance of this topic. The use of new technologies can lead to violations of the principles of international law and human rights, which requires the creation of preventive mechanisms within the framework of international law.* ***Discussion:*** *the relevance of the topic is also determined by the war situation in the world, which reminds us that against the backdrop of challenges in international law, there is a gap in terms of illegal integration of technologies in contemporary armed conflicts, which, as a result, leads to a breach of human rights and violation of the norms of both the Geneva Convention and the European Convention on Human Rights.*

Key words: *technology; war; IHL; human rights; UAVs; AI.*

Problem statement and its relevance. After the World War II, adoption of the new international norms significantly decreased the war statistics, however, in recent years, development of technologies, which was further accelerated by the pandemic, changed the mentioned statistics, to the extent that new technologies are actively used in war. Unfortunately, preventive and/or prohibitive international norms do not exist, therefore, we do not have the practice of regulating them. Paucity of regulative norms and the absence of proper literature in this field underscores the relevance of this topic. The use of new technologies can lead to violations of the principles of international law and human rights, which requires the creation of preventive mechanisms within the framework of international law. The relevance of the topic is also determined by the war situation in the world, which reminds us that against the backdrop of challenges in international law, there is a gap in terms of illegal integration of technologies in contemporary armed conflicts, which, as a result, leads to a breach of human rights and violation of the norms of both the Geneva Convention and the European Convention on Human Rights.

Summary of the main research material. *Legal Intersection of War and Technology (Practice of Ukraine).* Technology shapes warfare, not the

war, itself. The ICC has not investigate war crimes, committed by new technology, such as cyber attecks, AI, UAVs, autonomus weapons, etc. And do we have a possibiity to qualify them as a war crimes?

The omission of technological considerations within the definitions of war crimes outlined in various international treaties, including the Rome Statute, emphasizes a serious loophole in international legislation regarding of using new technological capabilities in modern warfare, therefore, new evolutionary definitions are needed.

While shaping the war crimes, all norms were defined as physical acts (willful killing, torture or inhuman treatment, etc.), however within the modern challenges, when the global digitalization is highly increasing, the actions taken in the digital space during the war can influence and change the dynamics and consequences of the war, therefore, it is necessary to take into account the cause-and-effect relations between the action and the result when qualifying, since the history of war development showed that technology was evolving along with the war.

Russian invasion of Ukraine was new puzzle for international community, they debated whether the mentioned armed conflict was a regular one or a new type of war. Mykhailo Fedorov, Ukraine's Minister of Digital Transformation, mentioned it as a «Technology war» and stated that technologies allow traditional and modern artillery to be more accurate, and they help save the lives of Ukrainian soldiers [1]. Palantir CEO Alex Karp stated that technology changes the competitive advantage of a small country over bigger one [1]. In the article of the Washington Post we can read «Russia and Ukraine are fighting the first full-scale drone war» [2].

This conflict is accelerating the implementation of fully autonomous drones and other weapons systems in the military, which has great influence on armed conflict and eventually changes the war statistics. Sinovation Ventures CEO Kai-Fu Lee said artificially intelligent weapons are third revolution in warfare after gunpowder and nuclear weapons [3].

What makes this conflict unique is the unprecedented willingness of foreign geospatial intelligence agencies to help Ukraine acquire satellite imagery and intelligence using artificial intelligence-enhanced systems. American companies play a leading role in this. Palantir Technologies was the first to provide its artificial intelligence software to analyze the course of war, determine the trajectory of troop movements and assess damage on the battlefield. Other companies such as Planet Labs, BlackSky Technology and Maxar Technologies also continuously produce satellite images of the conflict zone that are sent to the Ukrainian government and defense forces.

The Russia-Ukraine war can also be considered the first conflict where artificial intelligence-enhanced facial recognition software has been used substantially. In March 2022, the Ministry of Defense of Ukraine began using facial recognition software produced by the American company Clearview AI, which allows Ukraine to identify deceased soldiers [4], by July 2022, 7 agencies, and over 600 military personnel were actively using the Clearview AI platform, conducting over 60,000 searches. Each search had the potential to save a life at a checkpoint, help ID a missing person, and more [5]. This fact can be referred as a new era in international humanitarian law, since Ukraine protects not only the rights of soldiers, wounded, POWs and civilians according to Geneva Conventions, but also posthumous rights, that is one of the main challenges of IHL.

Autonomous and unmanned systems are considered the future of warfare. However, drones are already part of modern warfare. New technologies are changing the dynamics of war, if previously the big state would win because of the large territory, now the advantage holds the one who is more technologically advanced, however this fact, like everything else, requires some regulation. Ukraine proved that they are stronger than many analysts imagined. The conflict between Ukraine and Russia has shown how technology can play an important role in modern warfare.

Here are some technologies used in Ukraine:

Artillery and missile systems. In this conflict Russia used various types of artillery and missile systems, such as ballistic missiles, rocket launchers, and howitzers, Ukrainian-held territory and targets. By October 2022, more than 4,000 base stations,

60,000 km of fiber-optic lines, and 18 broadcasting antennas had been seized, damaged, or destroyed, according to Ukraine's Special Communications Service [6].

Drones. Ukraine war has featured more drone technology than any previous ones with using unmanned aerial vehicles (UAVs) for both, reconnaissance and surveillance. The Ukrainian military has also used drones to target enemy positions with munitions. The most used UAVs by Ukraine are commercial drones, with integrated high-resolution cameras that are paired with smartphones. Soldiers have used them for intelligence, surveillance, and reconnaissance, which puts them one step forward than their enemy. The Turkish Bayraktar TB2 drone is equipped with laser-guided bombs and is designed to target vehicles, troops, and military stations. Additionally, US-made Switchblade and Russian drones, also known as «Kamikaze drones», can be carried by a single person in a backpack. These drones have the capability to loiter and search for targets before crashing into them and detonating the warhead they carry. As the use of drones has become more prevalent in the conflict, both sides have also developed counter-drone systems to detect and neutralize enemy UAVs. The Ukrainian military has reportedly used anti-drone systems such as the Turkish-made KARGU drone, which can autonomously track and attack targets [7].

Artificial intelligence (AI). Military experts believe that AI will have a significant role in future conflicts, with AI systems being able to predict enemy movements and analyze vast amounts of data to detect potential threats. Dr. Nikos Loutas, NATO's head of data and AI policy, stated during the AI Summit London that the outcome of ongoing and future conflicts could be greatly influenced by the speed and effectiveness of AI, as well as which entities are utilizing AI on the battlefield. This highlights the importance of integrating AI technologies into military strategies to gain an advantage in warfare [8].

Apps. Mobile application and online portal Diia, which was launched in 2020 as a traditional government system used to help renew licensing permits, pay parking tickets, and report potholes, was repurposed to allow civilians to upload images and geolocation coordinates of different Russian military assets or to provide tips about suspicious people who might be collaborators, invaders, or saboteurs. Secure chat system eVorog («eEnemy») [9] was launched in March 2022 and has come to fore allowing civilians to provide multiple reports of different troop movements. The chatbot has transformed Ukrainian civilians with smartphones into digital resistance fighters by enabling them to collect and disseminate military intelligence effectively.

Deepfakes. On 16 March 2022, the Ukrainian TV channel Ukraine 24 appeared to have been hacked by pro-Russian hackers, leading to the broadcasting of a written message supposedly from President Zelensky calling for Ukrainian soldiers to surrender. That same day, deepfake videos using Volodymyr Zelensky's face were broadcast on the instant messaging system Telegram, promoting the same message that Ukrainian soldiers were to surrender to the Russian forces. This fake video was also published on several social media platforms, 11 including the Russian Vkontakte under the indirect supervision of the Kremlin [10].

Satellites. 5,000 Starlink satellite terminals were initially sent in the days after Russia's full-scale invasion. Keeping the Internet running has been critical to help Ukraine's citizens stay connected, but also to aide Ukraine's defensive coordination. Fedorov said at the time: «This is really the first major war in which commercially available satellite imagery may play a significant role in providing open-source information about troop movements, military build-ups in neighboring countries, flows of refugees, and more» [11].

Télécoms Sans Frontières (TSF). TSF is the world's first NGO focusing on emergency-response technologies and over the past 25 years, it has entered numerous humanitarian crises to give affected people the possibility to contact loved ones and begin to regain control of their lives, as well as build rapid-response communications centers for local and international responders. In response to the war in Ukraine, TSF teams reached Ukraine's neighboring countries to help refugees and also Ukraine itself to support displaced persons in Ukraine, providing emergency telecom equipment. Since the beginning of the conflict, over eight million refugees have left Ukraine seeking refuge and

six million are displaced within the country. That represents 32% of Ukraine's population [12].

3D Hologram. In June 2022, the President of Ukraine Volodymyr Zelensky made a 3D holographic broadcast appearance, powered by ARHT Media's holographic technology, to 200,000 top tech entrepreneurs, investors, and corporate leaders at seven major European tech events. He challenged tech leaders to donate financial and technological resources to begin rebuilding Ukraine. «Ukraine is a chance for a global digital revolution», he said: «a chance for every technology company and a chance for every visionary to show their value, skills, technologies, and ambitions» [13].

Social Medea. The war in Ukraine has become the most internet-accessible war in history with live updates and videos published through various social media platforms. Ukraine has been able to use social media location to be able to target specific groups of Russian soldiers. There has been a huge surge in social media activity too as friends and family members post updates and reach out to loved ones to inform them of their safety and whereabouts. Internet traffic coming back online in areas of Ukraine under Russian occupation have been re-routed to networks owned by the Russian government.

Cyberattack. Russia fired its first shots hours before the physical invasion started with repeated distributed denial of service (DDoS) attacks and a cyberweapon made up of a trojan horse wiper malware, which Microsoft identified and named as «FoxBlade», to attempt to knock out internet connectivity and paralyse Ukraine's command and control centers. The Anonymous hacker group quickly declared cyber war on the Russian government in response, whose FSB-created National Coordination Center for Computer Incidents (NCCC) classified the threat level as «critical» as there were reported failures for resources of the Ministry of Defense and the websites of the Kremlin, the government, parliaments, and parts of the Russia Today news agency [14]. 2,194 cyberattacks were witnessed in 2022, according to Yuriy Schygol, Head of the State Service for Special Communications and Information Protection of Ukraine, who said seven new types of virus had been identified [15].

It is notable that the development of technology has a great impact on the dynamics of war. In addition with old artillery system in the armed conflicts, artificial intelligence, drones, apps, social networks, satellites, cyberattacks, holograms and more were used. However, history is repeated again we do not have material norms, we still have no procedural norms and thereby imposing criminal liability to the perpetrators of international crime.

History is repeated, since crime against peace, nowadays, aggression, was even on the military tribunals, then it was formally recorded in the Roman status in 1998, and eventually ICC court shared its jurisdiction over this crime in 2017. As a result, we have left enforcement, or rather, untrained law against the perpetrators of aggression before 2017, as they have failed to agree on the definition, as well as the use of new technologies as an integral part of the war crime, though the international regulator and individual responsibility is nowhere to be seen.

LEGAL CHALLENGES OF CONTEMPORARY ARMED CONFLICT

Correct that, drone warfare is often referred to as a risk-free solution to international threats, however, the coin has two sides, and therefore there are negative expected consequences related to its use, which threatens one of the main values of the United Nations - international peace and security.

There are dozens of different types of drones, but in the war, they are used: 1. for intelligence and surveillance (e.g. the American RQ-4 Global Hawk; the British Watchkeeper WK450) and 2. with missiles and bombs (e.g. Turkish Bayraktar TB2, American MQ-9 Reaper).

Recently, USA has been actively using unmanned aerial vehicles (UAVs), over the past 20 years, the United States has carried out more than 93,000 airstrikes in Afghanistan, Iraq, Libya, Pakistan, Somalia, Syria and Yemen as a result of which 22,679 to 48,308 civilians have been killed [16]. USA has «Drone Laws» but this law is for commercial drones, not about the regulation of UAVs use as a weapon.

Unlike the USA, Britain takes the integration of AI in warfare more seriously, and to this end the British Ministry of Defense (MoD) is working on

ethical guidelines and issues of AI as a major military technology.

In 2022 MoD published a document called «Ambitious, Safe and Responsible» according to which «Artificial Intelligence (AI) as a family of general-purpose technologies, any of which may enable machines to perform tasks normally requiring human or biological intelligence, especially when the machines learn from data how to do those tasks» [17].

The minutes of the MoD AI Ethics Advisory Panel [18] showed that, despite of officials' attention on implementing AI programs and the ethical guidelines, AI is still in its infancy and requires several frameworks to become entirely safe.

As for Romano-Germanic law system, whose undeniable representative is Germany has more codified nature, codes in jurisdictions are laconic, amorphous, and created to solve problems even before they occur. For instance, the German Basic Law, according to which «peaceful relations between nations» [19] are protected by the Implementing Act to Article 26 (2) of the Basic Law (Act on the Control of War Weapons) [20]. The act lists the weapons of war, such as, objects, materials and organisms that might be used as one of the means of war between states, and therefore it can damage civilians or/and objects.

These weapons include nuclear weapons, biological weapons (e.g. harmful insects, biological agents, human, animal and plant pathogens), Chemical weapons (e.g. mustard gas) As well as other weapons of war, such as military aircraft or barrel guns. It should be noted that the direct term «drone» or «unmanned aerial vehicle» does not appear in this law, although the list includes combat aircraft if they have at least one of the following characteristics: 1. integrated weapon system, which in particular has target perception, fire control and corresponding interfaces to avionics, 2. integrated electronic warfare equipment, 3. Integrated electronic warfare system [21]. This law seems perfect for regulating autonomous weapons, but actually this law is about producing, licensing, transportation and purchase, therefore it cannot share its jurisdiction over autonomous weapons, UAVs, AI, etc.

At the level of the United Nations (UN), warnings from civil society have promoted multilateral talks about possible arms control for fully autonomous weapon systems, for which the UN term is LAWS (Lethal Autonomous Weapon Systems). These talks have been ongoing since 2014 within the framework of the UN Convention on Certain Conventional Weapons (CCW) in Geneva, according to which a weapon is considered fully autonomous if it completes the decision cycle for target engagement on its own, that is, after activation controlled solely by its software and without any human control or supervision, unlike a remotely controlled system. This targeting cycle includes the stages find, fix, track, target, engage and assess (abbreviated as F2T2EA). Fully autonomous weapons would thus be beyond human control when selecting and engaging targets actions that are especially sensitive from a legal, ethical and political point of view [22]. Mr. Sauer also gives us an example of fully autonomous weapon – Harpy, which is directed against radar installations and, for this limited purpose at least, it already goes through the targeting cycle without human control, and raises a question: who would be responsible if such systems cause civilian suffering that is disproportionate to the military value of the engagement, unjustifiable and therefore illegal [23]. Within the CCW, 26 countries are asking for prohibition of weapons operating without human control. But, of course, the US and Russia are strongly opposed to any kind of regulation.

Conclusions. Constat development of technologies, which was accelerated by the pandemic, changed war statistics, since new technologies, such as autonomous weapons, AI, UAVs, cyberattacks are actively used in armed conflicts. Unfortunately, there are not any international norms or national legislation which would regulate the use of above-mentioned technology in times of war, therefore, illegal integration of technologies in contemporary armed conflicts, leads to a breach of human rights and violation of the norms of both the Geneva Convention (IV) and the European Convention on Human Rights.

The conflict between Ukraine and Russia has shown how technology can play an important role in modern warfare, many soldiers and civilians

have died because of drone airstrikes, but international community cannot do anything, since there is not any prohibition.

Practice showed that over the past 20 years, the United States has carried out more than 93,000 airstrikes in Afghanistan, Iraq, Libya, Pakistan, Somalia, Syria and Yemen as a result of which 22,679 to 48,308 civilians have been killed, but no one is persecuted.

The omission of technological considerations within the definitions of war crimes outlined in various international treaties, including the Rome Statute, emphasizes a serious loophole in international legislation regarding of using new technological capabilities in modern warfare, therefore, new norm or evolutionary definitions are needed.

For these reasons, in order to avoid excessive damage, protect international peace and security and human rights, it is necessary, to adequately speed up the work of the UN on the definition of autonomous weapons, which will be included in the VI Additional Protocol to the Convention on the Prohibition of Certain Conventional Weapons (CCW).

References

1. Arhirova Hanna, Ukraine says it will beat Russia in the tech war 2023. URL: https://www.latimes.com/world-nation/story/2023-04-21/minister-ukraine-will-beat-russia-in-war-of-technologies.

2. Tech leaders are calling for an A.I., Lim Hui Jie 2023. URL: https://www.cnbc.com/2023/06/09/tech-leaders-ai-pause-no-product-ready-palantir.html.

3. Russia and Ukraine are fighting the first full-scale drone war, By Isabelle Khurshudyan, Mary Ilyushina and Kostiantyn Khudov, The Washington Post, 2022. URL: https://www. washingtonpost.com/world/2022/12/02/drones-russia-ukraine-air-war/.

4. Offer to assist Ukraine with facial recognition, Hoan Ton-That, 2022. URL: https://app.hubspot.com/documents/6595819/view/443117283?accessId=f27bac.

5. War in Ukraine, Clearview AI. URL: Ukraine - Clearview AI.

6. The Battle for Control Over Ukraine's Internet. URL: https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/.

7. Türkiye STM's Kargu kamikaze drones, 2023. URL: Japan eyes Türkiye STM's Kargu kamikaze drones (dsaexhibition.com).

8. NATO: Future conflicts may be won or lost by AI. URL: NATO: Future conflicts may be won or lost by AI (techinformed.com).

9. Ministry of Digital Transformation calls to use the eVorog through the Diia app. URL: https://www.kmu.gov.ua/en/news/mincifri-zaklikaye-koristuvatisya-yevorogom-cherez-zastosunok-diya.

10. Mazzucchi Nicolas, AI-based technologies in hybrid conflict: The future of influence operations, 2022, pp. 14-15. URL: https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf.

11. Commercial satellites test the rules of war in Russia-Ukraine conflict. URL: https://www. washingtonpost.com/technology/2022/03/10/ commercial-satellites-ukraine-russia-intelligence/.

12. Emergency response for the populations affected by the war. URL: https://www.tsfi.org/en/our-missions/disaster-response/ukrainian-crisis.

13. TNW: Zelensky hologram challenges tech leaders while Snowden gives bleak warning. URL: https://techinformed.com/tnw-zelensky-hologram-challenges-tech-leaders-while-snowden-gives-bleak-warning/.

14. The Hack of the Central Bank of Russia by Anonymous Group. URL: https://www.gizchina.com/2022/03/24/the-central-bank-of-russia-is-hacked-by-anonymous-group/.

15. Ukraine blames Russia for most of over 2,000 cyberattacks in 2022. URL: https://www.euronews.com/next/2023/01/17/ukraine-crisis-russia-cyber.

16. Thousands of civilians in Africa and the middle east have died as a result of America's use of unmanned aerial vehicles. URL: Thousands of civilians in Africa and the Middle East have died as a result of America's use of unmanned aerial vehicles - Foundation to Battle Injustice.

17. UK Ministry of Defense, Ambitious, Safe, Responsible - approach to the delivery of AI-enabled capability in Defense, UK, 2022 p.

18. Minutes of meetings of MoD's Ethical Advisory Panel. URL: https://dronewars.net/wp-content/uploads/2023/08/02-2020-04-06-FOI-AI-Ethics-Expert-Advisory-Panel-TORs.pdf.

19. Basic Law for the Federal Republic of Germany. URL: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0143.

20. Ausführungsgesetz zu Artikel 26 Abs. 2 des Grundgesetzes (Gesetz über die Kontrolle von Kriegswaffen). URL: https://www.gesetze-im-internet.de/krwaffkontrg/anlage.html.

21. Implementing Law to Article 26, Paragraph 2 of the Basic Law (Law on the Control of War Weapons), Annex (to Section 1 (1)) List of War Weapons, II. Combat aircraft and helicopters, 13. URL: https://www.gesetze-im-internet.de/krwaffkontrg/BJNR004440961.html#BJNR004440961BJNG000101305.

22. Sauer Frank, Artificial Intelligence in the Armed Forces On the need for regulation regarding autonomy in weapon systems, Security Policy Working Paper No. 26, 2018, pp. 1-4. URL: https://www.baks.bund.de/sites/baks010/files/working_paper_2018_26.pdf.

23. Basic Law for the Federal Republic of Germany. URL: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0143.

Ана Самакашвілі

ТЕХНОЛОГІЧНО-ПРАВОВІ ВИКЛИКИ СУЧАСНОГО ЗБРОЙНОГО КОНФЛІКТУ

Сухумський державний університет
вул. Анни Політковської, PPC5+6GG, Тбілісі, Грузія
E-mail: ana.samakashvili@sou.edu.ge

Мета статті: *дослідити взаємозв'язок між МГП, МКПЧ та нормами національного права та надати рекомендації щодо запобігання використанню технологій у сучасних збройних конфліктах.* ***Методи дослідження:*** *дослідження проведено порівняльно-правовим методом з метою представлення співвідношення міжнародно-правових та національних правових норм. Також ми використаємо нормативний метод, щоб підкреслити необхідність запровадження нових норм для врегулювання проблеми.* ***Результати:*** *після Другої світової війни прийняття нових міжнародних норм значно зменшило статистику війни, однак, в останні роки розвиток технологій, який ще більше прискорився пандемією, змінив згадану статистику настільки, що нові технології активно використовувався на війні. На жаль, превентивних та/або заборонних міжнародних норм не існує, тому у нас немає практики їх регулювання. Дефіцит регулятивних норм та відсутність належної літератури в цій галузі підкреслює актуальність даної теми. Використання нових технологій може призвести до порушення принципів міжнародного права та прав людини, що потребує створення превентивних механізмів у рамках міжнародного права.* ***Обговорення:*** *актуальність теми також визначається воєнною ситуацією у світі, яка нагадує нам, що на тлі викликів у міжнародному праві існує прогалина щодо незаконної інтеграції технологій у сучасні збройні конфлікти, яка, як в результаті призводить до порушення прав людини та порушення норм як Женевської конвенції, так і Європейської конвенції з прав людини.*

Ключові слова*: технології; війна; МГП; права людини; БПЛА; ШІ.*

Стаття надійшла до редакції 29.08.2024